E-SAFETY POLICY

(Academies)

The OHC&AT Board of Directors has agreed this Policy and as such, it applies across all OHCAT Academies – 15th December 2017.
Jay Mercer
Chair of OHCAT Board

E-Safety Policy

INTRODUCTION

Orchard Hill College and Academy Trust (OHC&AT) is committed to providing outstanding educational opportunities for all our pupils and students. The safety and welfare of our pupils and students is of the utmost importance. Ensuring that pupils and students can safely access new technology and learn how to participate in the digital world without compromising their safety and security is a key part of delivering a well-rounded programme of education.

This policy sets out how we will keep pupils/students at OHC&AT Academies safe, whether using new technology within OHC&AT provision or at home. There is a separate policy for Orchard Hill College.

This policy has been written with reference to the London Grid for Learning (LGfL) E-Safety Policy, the South West Grid for Learning (SWGFL) E-Safety Policy, Ofsted's Inspecting E-safety in Schools (April 2014) and the NUT Policy on E-safety. The policy is also informed by government guidance on the Prevent duty and Channel. E-safety represents a crucial strand of safeguarding children and vulnerable adults, and such this policy cross-references to OHC&AT's Child Protection and Safeguarding Policy and Procedures.

This policy applies to all members of the OHC&AT community including staff, pupils/students, volunteers, parents and carers, visitors, outside professionals and community users who have access to OHC&AT's ICT system.

E-SAFETY IN ACADEMIES

The impact of technology on the lives of all citizens increases yearly, particularly for children and young people who are keen to explore new and developing technologies. Technology is transforming the way that schools teach and children learn. At home, technology is changing the way children live and the activities in which they choose to partake. Developing technology brings opportunities; it also brings risks and dangers including:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to, loss of, and sharing of personal information
- Internet grooming
- Radicalisation
- The sharing and distribution of personal images without consent
- Inappropriate communication and contact with others
- Cyber-bullying
- Sexting
- Access to unsuitable video and internet games

- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- Excessive use which may impact on social and emotional development and learning

ROLES AND RESPONSIBILITIES

Each OHC&AT Academy has a named E-Safety Lead, who will oversee and manage the recording, investigation and resolution of cyberbullying and any other incidents which fall within the remit of this policy.

All OHC&AT staff will familiarise themselves with this policy. E-safety is included in discrete lessons, training to staff and also throughout the year through other vehicles, such as assemblies.

Each OHC&AT Academy has a Governor responsible for Safeguarding and Child Protection, who will monitor adherence to the policy, together with the E-Safety Lead, and feedback to the Local Governing Body as appropriate.

OHC&AT Academies will monitor the impact of this policy using:

- Logs of reported incidents (maintained by the E-Safety Lead).
- Monitoring of the Academy's network where necessary.
- Regular monitoring of the Academy's social media presence.
- Monitoring of the Academy's Google Apps platform where necessary.
- Monitoring of the Academy's internet access where necessary, and regular reviews of the Academy's website filtering.
- Parent/carer questionnaires.

CREATING A SAFE ICT INFRASTRUCTURE

All users of OHC&AT Academy computer networks have clearly defined access rights, enforced using a username and password login system. Account privileges are achieved through the file and folder permissions, and are based upon each user's requirements. Pupils' accounts are restricted and do not allow access to all network drives. Guests are required to login using a visitor login that has limited network access.

A permanently-enabled filtering system is used to filter inappropriate material. Additionally web pages are scanned for content as requested. Any changes to setting have to be requested through the OHC&AT IT Helpdesk. All changes made to Internet filtering are logged. Security software is installed on all computers.

Staff should be aware that Internet traffic is monitored and can be traced to the individual user. It is the responsibility of the user to ensure that they have logged off

the system when they have completed their task and to keep their user credentials confidential.

Please refer to the OHC&AT IT Acceptable Use Policy for further details.

Rules for publishing material online (including images of pupils)

Academy websites are a valuable tool for sharing information and promoting pupils' and students' achievements. We recognise the potential for abuse. Therefore the following principles will always be considered:

- If an image, video or audio recording of a pupil/student is used, their surname should not be used (including in credits).
- Staff **must not** take photographs of pupils or students using their personal devices – all pupil/student photographs must be taken using OHC&AT equipment.
- Files should be appropriately named in accordance with these principles.
- Only images of pupils/students in suitable dress should be used and group photographs are preferred (though not exclusively) in preference to individual photographs.
- Parents/carers are given the opportunity to withdraw permission for the Academy to publish images/audio/video of their child on the Academy website.
- Content should not infringe the intellectual property rights of others – copyright may apply to text, images, music or video that originate from other sources. All copied or embedded content should be properly referenced.
- Content should be polite and respect others.
- Material should be proofread by a member of the Academy's Senior Leadership Team before being published.

Children and young people use a variety of online tools for educational purposes. They will be asked to only use their first name or a suitable avatar for any work that will be publicly accessible and will be required to follow the principles listed above before sending any work for publishing. Staff should encourage contributions that are worthwhile and develop a particular discussion topic.

When photos and videos of Academy events are permitted to be taken by parents and carers, they will be asked not to publish them on any public area of the Internet, including social networking sites.

Pupil/student rules for acceptable internet use

We will adopt the rules as laid out below in an age-appropriate way for the pupils/students at OHC&AT Academies.

- *I will ask permission from an adult before using the Internet.*
- *I will use computers and tablets safely.*
- *I will not look for websites that I know I'm not allowed to see.*
- *If I see anything that I know is wrong I will tell an adult straight away.*

- *I will not download anything without permission from an adult.*
- *I will not use memory sticks on school computers without permission from an adult.*
- *I will ask an adult before sending emails.*
- *I will be polite and respect others when using the Internet.*
- *I will not give out any personal information over the Internet.*
- *I will not share my login details with others.*
- *I understand that the school may check my computer files and check what I am doing.*

Visitor rules for acceptable internet use

Visitors' Internet use will vary depending upon the purpose of their visit. Generally we expect all visitors to abide by the following rules:

- *I will respect the facilities by using them safely and appropriately.*
- *I will not use the Internet for personal financial gain, political purposes, advertising, personal or private business.*
- *I will not deliberately seek out inappropriate websites.*
- *I will report any unpleasant or upsetting material to a member of staff immediately.*
- *I will not download or install program files.*
- *I will not use USB memory devices on Academy computers.*
- *I will be polite and respect others when communicating over the Internet.*
- *I will not share my login details.*
- *I will not carry out personal or unnecessary printing.*
- *I understand that the Academy may check my computer files and monitor my Internet use.*

Staff and Governor rules for acceptable internet use

Staff and governors must use the Internet safely, appropriately and professionally within the Academy. They must be aware that they are role models for others and should promote and model high standards of behaviour at all times. For further details please refer to the OHC&AT IT Acceptable Use Policy.

E-SAFETY EDUCATION AND TRAINING

The aim of e-safety education within OHC&AT Academies is to teach pupils and students how to manage and deal with risks they encounter by themselves, whilst at the same time encouraging them to become positive users of both new and emerging technologies.

Pupils/students will be taught about safe and appropriate electronic communication, including the indelible nature of emails, social media presence, images and other e-communications. Aspects of e-safety such as cyberbullying, revenge porn, trolling and other harassment will be covered in an age-appropriate way, with emphasis placed on

respecting oneself and one's peers, in order to build confidence and understanding among pupils/students as they interact with technology.

For younger pupils/students Internet use will be closely supervised and based around pre-selected, safe websites. Pupils/students will be regularly reminded about how to always take care when clicking and to seek help from an adult if they see anything that makes them unhappy or that they are unsure about. These digital literacy skills will be developed in keeping with pupils'/students' age and ability, with lessons promoting a responsible attitude towards searching the Internet and the importance of personal security measures such as strong passwords and processes for reporting any concerns.

As they progress through the Academy, pupils/students will be encouraged to become more independent at researching information on the Internet, being taught the necessary skills to critically evaluate sites for accuracy and suitability. They will be supported to use online collaboration tools for communicating and sharing ideas.

E-safety updates for staff

Staff will receive regular updates about how to protect and conduct themselves professionally online and to ensure that they have an awareness of issues surrounding modern technologies, including safeguarding. They are also directed to relevant websites to help support their understanding of these issues. Some of this information will be provided by email updates and at staff meetings.

E-safety updates for parents/carers

OHC&AT aims to provide opportunities for parents and carers to receive e-safety education and information (e.g. via the Academy website and/or newsletters) to enable them to better understand the issues surrounding new technologies and to help them support their children in developing good e-safety.

Guidance on the use of social networking and messaging systems

OHC&AT recognises that many staff will actively use Facebook, Twitter and other social networking, blogging and messaging services, including to support their own professional development by developing personal learning networks with other educational practitioners.

Staff must recognise that it is not appropriate to discuss issues relating to pupils/students or colleagues via social media networks; discretion and professional conduct is essential. Posts that bring OHC&AT into disrepute and/or breach confidentiality are likely to result in disciplinary action. Staff should review their privacy settings to make sure that their profiles and photographs are not viewable by the general public.

It is never acceptable to accept a friendship request from a child or young person in an OHC&AT provision or from ex-pupils/students who are still minors. This is to avoid

any possible misinterpretation of motive or behaviour which could be construed as grooming.

Staff must not give their personal contact details to pupils/students, including e-mail, home or mobile telephone numbers. All correspondence should be via OHC&AT systems.

DATA PROTECTION

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse;
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly 'logged-off' or 'locked' at the end of any session in which they are using personal data;
- Be fully aware of the risks of transferring data using removable media. When personal data is stored on any portable computer system, USB stick or any other removable media, it must be securely deleted once its use is complete.

It may sometimes be necessary to send confidential information outside the organisation e.g. as part of a safeguarding investigation. **OHC&AT staff must at all times consider the security of such information.** Any confidential or sensitive information conveyed via email must be password protected and the password conveyed separately to the recipient, preferably by means other than email. Confidential or sensitive emails should be encrypted wherever possible.

POLICY REVIEW DETAILS

Version:	1.1
Reviewer:	Janet Sherborne, John Prior
Approval body:	Family Board
Date this version approved:	15th December 2017
Due for review:	Autumn 2020

RELATED POLICIES AND PROCEDURES

Child Protection Safeguarding Policy and Procedures
IT Acceptable Use Policy
Data Protection Policy
Staff Code of Conduct
Anti-Bullying Policy
Anti-Radicalisation Policy
Dignity at Work Policy

APPENDIX 1: How to Stay 'Cybersafe' – Staff Do's and Don'ts

DO

- Be aware of your online reputation, which consists of information you post about yourself and information posted by others, and consider that when seeking employment, many prospective employers will use publicly available online information. Remember, the internet never forgets.
- Keep passwords confidential and protect access to accounts.
- Regularly review your privacy settings.
- Discuss expectations with friends – are you happy to be tagged in photos, for example?
- Be aware that, increasingly, individuals are being held to account in the Courts for the things they say on social networking sites.
- Keep personal phone numbers private and don't use your own mobile phones to contact pupils/students or parents/carers.
- Use an OHC&AT mobile phone for OHC&AT business.
- Keep a record of your phone's unique International Mobile Equipment Identity (IMEI) number, keep phones secure while on Academy premises and report thefts to the police and mobile operator as soon as possible.
- Ensure that Academy rules regarding the use of technologies are consistently enforced.
- Report any incident to the appropriate member of staff in a timely manner.
- Keep any evidence of an incident, for example by not deleting text messages or emails and by taking a screen capture of material, including the URL or web address.
- Use your OHC&AT email address only for work purposes.
- Be aware that if you access any personal web-based email accounts via the OHC&AT network, these may be subject to the Academy's internet protocol which could include monitoring and surveillance.
- Raise genuine concerns about your Academy or specific members of staff using whistle blowing or grievance procedures.

DON'T

- Post information and photos about yourself, or OHC&AT-related matters, publicly that you wouldn't want employers, colleagues, pupils/students or parents/carers to see.
- Befriend pupils/students or other members of the school community on social networking sites. (You should consider carefully the implications of befriending parents/carers or ex-pupils/students and let the SLT at your Academy know if you decide to do this.)
- Personally retaliate to any incident or bullying messages.
- Criticise your Academy, OHC&AT, pupils/students or parents/carers online.